

87

Notice of Allowability

Application No.

09/849,697

Examiner

Grigory Gurshman

Applicant(s)

LINGAFELT ET AL.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed 6/29/2005.
2. ☒ The allowed claim(s) is/are 1-3, 7, 8, 10-12, 15, 17-19 and 22-30.
3. ☒ The drawings filed on 04 May 2001 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date <u>7/26/2005</u> . |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____ |

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Joe Christian on 7/26/2005.

The application has been amended as follows:

Claim 1 : A method enabling a network-addressable device to detect use of its identity by a spoofing vandal, comprising the acts of:

receiving a message by the network-addressable device from a target of a denial of service-attack by the spoofing vandal, said attack comprising a denial of service communication sent by the spoofing vandal to the target;

detecting, by the network-addressable device, a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of the denial of service attack on the target by the spoofing vandal using an identity of the network-addressable device in the denial of service communication, ~~said~~ the detecting of the communication protocol violation, being performed after ~~said~~ the receiving of the message by the network-addressable device has been performed; and

generating, by the network-addressable device, a spoofing alert responsive to the act of detecting the communication protocol violation.

Claim 22: A method enabling a network-addressable device to detect use of its identity by a spoofing vandal, comprising the acts of:

receiving a message by the network-addressable device from a target of a denial of service attack by the spoofing vandal, said attack comprising a denial of service communication sent by the spoofing vandal to the target;

detecting, by the network-addressable device, a communication protocol violation consequent to the message, wherein the communication protocol violation is indicative of the denial of service attack on the target by the spoofing vandal using the identity of the network-addressable device in the denial of service communication, ~~said~~ the detecting of the communication protocol violation being performed after ~~said the~~ receiving of the message has been performed;

recording attributes of the message;

advancing the value of a counter associated with the target;

comparing the value of the counter with a predetermined threshold;

generating a spoofing alert when a result of said comparing is that the value of the counter exceeds the threshold, said recording, advancing, comparing, and generating being performed by the network-addressable device.

Allowable Subject Matter

2. Claims 1-3, 7-8, 10-12, 15, 17-19, 22-30 are allowed.

3. The following is an examiner's statement of reasons for allowance:

3.1 Referring to the independent claims 1 and 22, Sherer discloses a medium access control address authentication (see abstract and Fig. 4). Sherer teaches a plurality of ports adapted for connection to respective MAC layer devices includes storing authentication data in the star configured interconnection device that maps MAC addresses of end stations in the network to particular ports on the star configured interconnection device. Upon receiving a packet on a particular port, the process involves determining whether the packet carries a source address, which the authentication data maps to the particular port. If the packet carries a source address, which the authentication data maps to the particular port, then the packet is accepted. If the packet does not carry a source MAC address, which the authentication maps to the port, then an authentication protocol is executed on the port to determine whether the MAC address originates from an authorized sender according to the authentication protocol (see abstract). According to Sherer, network devices learn the segments of the network on which to find certain MAC addresses. Thus, by using the MAC address of another device, an end station is capable of fooling the network so that packets destined to the end station that it is mimicking, are routed to the mimic. An unscrupulous user spoofing another packet can introduce unwanted data such as computer viruses

Art Unit: 2132

into a packet stream being transmitted from the end station, or hijack a user's network session and gain unauthorized access to other system resources (see column 1, lines 50-65).

3.2 Sherer, however, does not teach detecting, by the network-addressable device, a communication protocol violation indicative of the denial of service attack on the target by the spoofing vandal using an identity of the network-addressable device in the denial of service communication.

Referring to the independent claims 1 and 22, Glawitsch discloses a system for preventing spoofed denial of service attack in networked computing environment (see abstract). Glawitsch teaches generating a request acknowledgement packet with checksum as pseudo sequence number and source address in request packet as destination address. Comparison of the check sums serves as indication of the denial of service attack (see abstract and Fig. 8). Glawitsch, however, does not teach or suggest *the denial of service attack on the target by the spoofing vandal using an identity of the network-addressable device*.

3.3 Neither Sherer nor Glawitsch teach or suggest generating by the network-addressable device a spoofing alert. Referring to the instant claim, Franz teaches generating spoof control packet, setting the alerts and discarding the packets (see abstract and Fig. 3, blocks 340 and 399). However, combination of Sherer with Glawitsch and with Franz does not render the instant claims obvious, because of the deficiencies of Sherer and Glawitsch indicated above (see paragraph 3.1-.3.2).

4. In view of the reasons presented herein, claims 1-3, 7-8, 10-12, 15, 17-19, 22-30 are in condition for allowance.

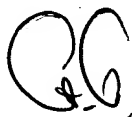
Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

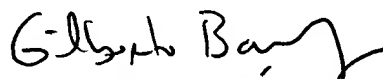
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Grigory Gurshman whose telephone number is (571)272-3803. The examiner can normally be reached on 9 AM-5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Grigory Gurshman
Examiner
Art Unit 2132



GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100